

Quantum No-Stretching: a geometrical interpretation of the No-Cloning Theorem

Giacomo M. D'Ariano^{a,b}, Paolo Perinotti^{a,b}

^a*QUIT Group, Dipartimento di Fisica "A. Volta", via Bassi 6, I-27100 Pavia, Italy*

^b*Istituto Nazionale di Fisica Nucleare, Sez. di Pavia, via Bassi 6, I-27100 Pavia, Italy*

Abstract

We consider the ideal situation in which a space rotation is transferred from a quantum spin j to a quantum spin $l \neq j$. Quantum-information theoretical considerations lead to the conclusion that such operation is possible only for $l \leq j$. For $l > j$ the optimal stretching transformation is derived. We show that for qubits the present No-Stretching theorem is equivalent to the usual No-Cloning theorem.

Key words: quantum information, no-go theorems, spin, spatial rotations

PACS: 03.67.-a

“No-go” theorems [1] play a crucial role in Quantum Information Theory [2] and for foundations of Quantum Mechanics [3]. Among the no-go theorems, the celebrated No-Cloning [4, 5, 6, 8, 9, 7] is considered the starting point of the field of Quantum Information itself, lying at the basis of security of quantum cryptography. Other relevant no-go theorems are the No-Programming Theorems [2, 10, 11, 12], and the No-Universal-NOT [13, 14]. The No-Cloning Theorem states the impossibility of building a machine that produces perfect clones of the same unknown quantum state. The No-Programming Theorems state the impossibility of building a machine that can perform any desired quantum operation or POVM (positive-operator-valued measure) which is programmed in a quantum register inside the machine. Finally, the No-Universal-NOT states the impossibility of building a device that reverses a qubit in any unknown quantum state.

Email addresses: dariano@unipv.it (Giacomo M. D'Ariano),
perinotti@fisicavolta.unipv.it (Paolo Perinotti)

URL: www.qubit.it (Giacomo M. D'Ariano), www.qubit.it (Paolo Perinotti)

The proofs of the No-Cloning and no-programming theorems have a common feature: in both cases the pertaining ideal transformation should map pure states to pure states, i. e. it *does not entangle* the system with the machine. Therefore, if one supposes that the transformation is described by a unitary evolution U , as dictated by Quantum Mechanics, the input quantum state ψ is transformed to ψ' as follows

$$U|\psi\rangle|\eta\rangle = |\psi'\rangle|\eta'(\psi)\rangle, \quad (1)$$

with an auxiliary system (which can be part of the machine, but may also include the environment) prepared in a *reset state* η and ending up in a state $\eta'(\psi)$ generally depending on ψ . The argument of the impossibility proof is then to derive a contradiction by considering the scalar product between different states at the input and at the output [6, 15]

$$\langle\phi|\psi\rangle = \langle\phi'|\psi'\rangle\langle\eta'(\phi)|\eta'(\psi)\rangle, \quad (2)$$

and for $|\langle\phi'|\psi'\rangle| < |\langle\phi|\psi\rangle|$, since $|\langle\eta'(\phi)|\eta'(\psi)\rangle| \leq 1$ one has an overall reduction of the scalar product, which contradicts the supposed unitarity. In information theoretical terms a decrease of the scalar product means an increased state-distinguishability, which would lead to a violation of the classical data-processing theorem by the machine regarded as an input-output communication channel.

We will now see that this situation occurs in another no-go theorem—which we will refer to as *No-Stretching Theorem*—which *forbids stretching a spin while keeping its unknown orientation*. In other words, it is impossible to transfer a spatial rotation from a spin j to a larger spin $l > j$. For a more general transformation group the situation is more complicated, because the labels for irreducible representations are usually vectors rather than (half)integers, and one must find conditions on couples of such vectors under which transfer from one irrep to another is impossible. Increasing dimension of the space carrying the representation is not a sufficient criterion for impossibility, as one could easily prove considering the impossibility of covariantly transforming the representation U for $SU(d)$ to its complex conjugate U^* , which is carried by a space with the same dimension d [16]. As we will see in the following, it is not just the angular momentum conservation that matters, since the transfer of rotation is possible when the spin is decreased to $l < j$.

Let us consider a spin j prepared in the coherent state for the angular momentum $U_g^{(j)}|j, j\rangle$ with g a generic unknown element of the group $SU(2)$.

The state $|j, j\rangle$ is chosen, with the angular momentum pointing toward the north pole—however, any other initial direction would be equivalent. The task is now to transfer the spatial rotation from the spin j to a different spin $l \neq j$, namely to get the state $U_g^{(l)}|l, l\rangle$. If such transfer were physically feasible there would exist a unitary transformation W such that

$$W(U_g^{(j)}|j, j\rangle \otimes |E\rangle) = U_g^{(l)}|l, l\rangle \otimes |\theta(g)\rangle, \quad (3)$$

where $|E\rangle$ is the reset state of the spin-stretching machine, and $|\theta(g)\rangle$ is a machine state depending on g [Notice that these states belong to spaces of different dimensions, since $j \neq l$. For example one could take $|E\rangle = |l, l\rangle \otimes |\omega\rangle$, $|\omega\rangle$ the reset state of an additional ancilla, and then transfer the unitary rotation U_g from the spin j to the spin l .] By taking the scalar product between vectors rotated with a different g , one has

$$\langle j, j|U_h^{(j)\dagger}U_g^{(j)}|j, j\rangle = \langle \theta(h)|\theta(g)\rangle \langle l, l|U_h^{(l)\dagger}U_g^{(l)}|l, l\rangle. \quad (4)$$

The matrix element of the transformation is just a function of the second Euler angle β of the rotation $h^{-1}g$ (see Ref.[17])

$$\langle x, x|U_h^{(x)\dagger}U_g^{(x)}|x, x\rangle = \left(\cos \frac{\beta}{2}\right)^{2x}, \quad x = j, l, \quad (5)$$

whence it is a decreasing function of x , since $0 < |\cos \frac{\beta}{2}| < 1$ (for non-parallel and non-orthogonal states, i. e. $\beta \neq k\pi$, k integer). Then, in order to preserve the overall scalar product, for $j < l$ we must have $|\langle \theta(h)|\theta(g)\rangle| > 1$, which is impossible, whereas for decreasing spin $j > l$ we must have $|\langle \theta(h)|\theta(g)\rangle| < 1$, which is allowed by quantum mechanics.

We call the above no-go theorem *no-stretching*, since it forbids to transfer a spatial rotation to a larger spin. In physical terms, as can be intuitively understood by figuring a spin as a vector, this theorem forbids to amplify a signal corresponding to a spatial rotation by enlarging the vector which is rotated, whereas it is in principle possible to shorten the vector (as shown in detail in the following), attenuating the signal (see Fig. 1).

If we cannot stretch the spin by keeping the same unknown orientation, we can anyway try to do our best to keep the orientation by blurring the state of the spin toward a mixed one. What is then the *optimal physical stretching map*, which transfers the rotation g from a spin j to a spin $l \neq j$ optimally, e. g. with the maximum state-fidelity? For $j < l$ such fidelity

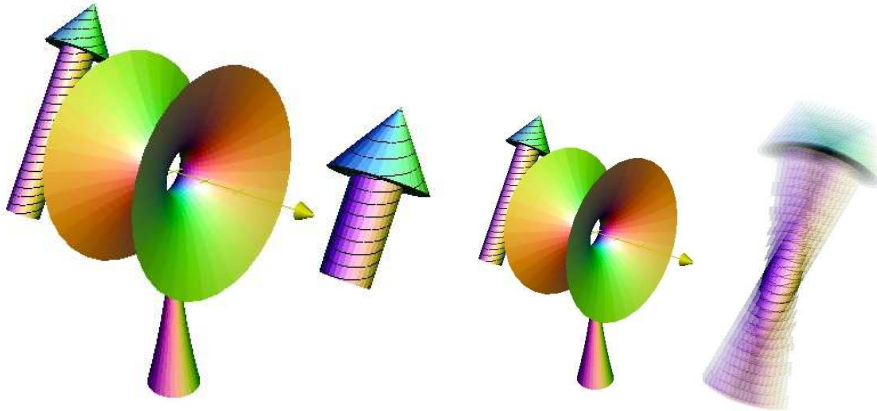


Figure 1: The No-Cloning theorem of Quantum Mechanics is actually a special case of *no-stretching theorem*, which asserts that unitary transformations cannot be “amplified” to unitaries carrying more information about the parameter of the group element, making two nonorthogonal states more “distinguishable”. For example, there is no machine that takes a rotated eigenstate of the z -component of the angular momentum and produces an output larger angular momentum rotated in the same way. In the figure we pictorially represent the no stretching theorem. While it is possible to output a rotation exactly from a spin j to a shorter spin $l < j$ (figure on the top), the same operation cannot be achieved exactly when the second spin is larger $l > j$ (figure on the bottom). In the latter case the direction is blurred in form of a mixing of the output state.

must be certainly smaller than one, whereas for $j > l$ we expect that it can be unit. In technical terms, in order to be physically achievable the optimal map must be: 1) completely positive (CP)—namely it must preserve positivity also when applied locally on the system entangled with an ancilla; 2) trace-preserving; 3) *rotation-covariant*, corresponding to the request that the map transfers the spin rotation. Mathematically, upon denoting the map as $\rho_l = \mathcal{M}(\rho_j)$ acting on a state ρ_j of the spin j and resulting in a state ρ_l of the spin l , the covariance of the map is translated to the identity

$$\mathcal{M}(U_g^{(j)} \rho_j U_g^{(j)\dagger}) = U_g^{(l)} \mathcal{M}(\rho_j) U_g^{(l)\dagger}. \quad (6)$$

The CP condition is equivalent to the possibility of writing the map in the Kraus form [18]

$$\mathcal{M}(\rho) = \sum_k M_k \rho M_k^\dagger. \quad (7)$$

where M_k are linear operators from the input Hilbert space \mathcal{H}_{in} to the out-

put Hilbert space \mathcal{H}_{out} . The trace-preserving condition corresponds to the constraint $\sum_k M_k^\dagger M_k = I$. Optimality is defined in terms of maximization of the input-output fidelity

$$F := \langle l, l | \mathcal{M}(|j, j\rangle\langle j, j|) | l, l \rangle. \quad (8)$$

The following Kraus operators M_k give the optimal map \mathcal{M}

$$\begin{aligned} M_k &= s_{jl} \sum_{m \in I_k} |l, m+k\rangle \langle j, m| \langle j-l, k; j, -m, l, m+k| \\ &= s_{jl} \sum_{m \in J_k} |l, m\rangle \langle j, m-k| \langle j-l, k; j, -m+k, l, m\rangle, \end{aligned} \quad (9)$$

where $I_k = [-j, j] \cap [-l-k, l-k]$, $J_k = [-l, l] \cap [-j+k, j+k]$, and

$$s_{jl} = \sqrt{\frac{2j+1}{2|j-l|+1}} \quad (10)$$

where $-|j-l| \leq k \leq |j-l|$, $\langle J, M; j, m, l, n \rangle$ denotes the Clebsch-Gordan coefficient [17] for the coupling between the two spins j and l into their sum J . The Clebsch-Gordan coefficients in Eq. (9) guarantee both trace preservation and covariance. The above map has been obtained by standard optimization techniques based on convex analysis. In particular, we used the Choi-Jamiolkowski representation [19, 20] for CP maps, which exploits the following one-to-one correspondence between CP maps \mathcal{M} from \mathcal{H}_{in} to \mathcal{H}_{out} and positive operators $R_{\mathcal{M}}$ on $\mathcal{H}_{\text{out}} \otimes \mathcal{H}_{\text{in}}$

$$R_{\mathcal{M}} = \mathcal{M} \otimes \mathcal{I}(|\Omega\rangle\langle\Omega|), \quad \mathcal{M}(\rho) = \text{Tr}_{\text{in}}[(I_{\mathcal{H}_{\text{out}}} \otimes \rho^T) R_{\mathcal{M}}], \quad (11)$$

where $|\Omega\rangle := \sum_{j=1}^d |\psi_j\rangle |\psi_j\rangle$ is a maximally entangled state, with $d := \dim(\mathcal{H}_{\text{in}})$, the symbol $\text{Tr}_{\text{in/out}}$ denotes the partial trace on the Hilbert space \mathcal{H}_{in} (\mathcal{H}_{out} , respectively), and ρ^T is the transpose of the state ρ on the orthonormal basis $\{|\psi_j\rangle\}$. Trace preservation is guaranteed by the condition $\text{Tr}_{\text{out}}[R_{\mathcal{M}}] = I_{\mathcal{H}_{\text{in}}}$. The covariance property Eq. (6) translates to the following commutation property for $R_{\mathcal{M}}$ [21]

$$[(U_g^{(l)} \otimes U_g^{(j)*}), R_{\mathcal{M}}] = 0, \quad \forall g \in \text{SU}(2). \quad (12)$$

Now, it is easy to verify that trace preservation, CP and covariance properties are all preserved under convex combination of different maps, which by linearity of Eqs. (11) corresponds to convex combination of Choi-Jamiolkowski

operators. Since the fidelity (8) is linear versus \mathcal{M} and the set of covariant CP trace-preserving maps is convex, the optimal map is an extremal point of such set, namely it cannot be written as a convex combination of any couple of different maps. Our analysis consists in classifying extremal points of the set of covariant maps and then looking for the optimal one.

The derivation of the optimizal map is quite technical, however, it is easy to check optimality. Consider the case $j > l$. Then we have $|j - l| = j - l$. Applying the map to the state $|j, j\rangle$ and using elementary properties of the Clebsch-Gordan coefficients we obtain

$$\mathcal{M}(|j, j\rangle\langle j, j|) = |l, l\rangle\langle l, l|. \quad (13)$$

This proves that the ideal map is exactly achievable for $j > l$. On the other hand, for $j < l$ we have $|j - l| = l - j$, and the output of the map applied to $|j, j\rangle$ in this case is

$$\begin{aligned} \mathcal{M}(|j, j\rangle\langle j, j|) = \\ \frac{2j+1}{2l+1} \sum_{k=j-l}^{l-j} \frac{(2l-2j)!(l+j+k)!}{(2l)!(l-j+k)!} |l, k+j\rangle\langle l, k+j|. \end{aligned} \quad (14)$$

The fidelity is easily evaluated as

$$F = \frac{2j+1}{2l+1}, \quad (15)$$

with plot given in Fig. 2.

The optimality of the fidelity (15) can be proved as follows. The optimal measurement of the spin direction is described by the covariant POVM obtained in Ref. [22]

$$P_g^{(j)} dg = (2j+1) dg U_g^{(j)} |j, j\rangle\langle j, j| U_g^{(j)\dagger}, \quad (16)$$

with group integrals normalized as $\int_{\mathbb{SU}(2)} dg = 1$. This is the POVM that maximizes the likelihood

$$L := \langle j, j | P_e^{(j)} | j, j \rangle, \quad (17)$$

of the covariant estimation of $\mathbb{SU}(2)$ elements on the vector $|j, j\rangle$ [22], and the maximum likelihood is $2j+1$. Notice that the POVM in Eq. (16) minimizes

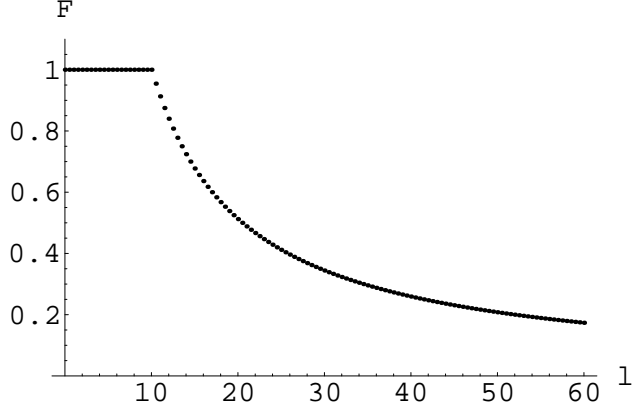


Figure 2: Fidelity of the optimal spin-stretching map for $j = 10$ as a function of l .

all cost functions in the generalized Holevo class [23]. We now evolve this POVM with our map \mathcal{M} with Kraus operators given in Eq. (9). This corresponds to apply the dual map \mathcal{M}^* in the reverse order, i. e. from spin l to j , corresponding to the Heisenberg picture (in which we evolve operators instead of states). We thus obtain

$$\mathcal{M}^*(P_g^{(l)}) = (2l+1)U_g^{(j)}\mathcal{M}^*(|l,l\rangle\langle l,l|)U_g^{(j)\dagger}. \quad (18)$$

The likelihood of such POVM is

$$\begin{aligned} L &= (2l+1)\langle j,j|\mathcal{M}^*(|l,l\rangle\langle l,l|)|j,j\rangle = \\ &= (2l+1)\langle l,l|\mathcal{M}(|j,j\rangle\langle j,j|)|l,l\rangle = (2l+1)F \leq 2j+1, \end{aligned} \quad (19)$$

and the optimal map saturates this bound.

By using the same POVM we can prove that the optimal map preserves the classical information about the spatial rotation. In order to prove this statement, let us consider the Kraus operators in Eq. (9). Using the identity for the Clebsch-Gordan coefficients

$$\langle |j-l|, k; j, -m, l, m+k \rangle = \langle |j-l|, -k; l, -m-k, j, m \rangle, \quad (20)$$

and renaming $n = m+k$, the Kraus operators of the dual map $\mathcal{M}^* =$

$\sum_k M_k^\dagger \cdot M_k$ can be rewritten as follows

$$\begin{aligned}
M_k^\dagger &= s_{jl} \sum_{m \in I_k} |j, m\rangle \langle l, k+m| \langle j-l, k; j, -m, l, k+m| \\
&= s_{jl} \sum_{n \in J_k} |j, n-k\rangle \langle l, n| \langle j-l, k; j, k-n, l, n\rangle \\
&= s_{jl} \sum_{n \in J_k} |j, n-k\rangle \langle l, n| \langle j-l, -k; l, -n, j, -k+n\rangle.
\end{aligned} \tag{21}$$

Considering that $s_{lj} = \sqrt{\frac{2l+1}{2j+1}} s_{jl}$, it is now immediate to notice that the dual map \mathcal{M}^* for the case $l > j$ coincides with the direct map for input spin l and output j , apart from a multiplicative constant $\frac{2j+1}{2l+1}$, since the Kraus operator M_k^\dagger of \mathcal{M}^* coincides with the Kraus operator M_{-k} of \mathcal{M} from l to j . Then,

$$(2l+1)\mathcal{M}^*(|l, l\rangle \langle l, l|) = (2j+1)|j, j\rangle \langle j, j|. \tag{22}$$

This implies that the conditional probability distribution

$$p(g|h) = \text{Tr}[P_g^{(l)} \mathcal{M}(U_h^{(j)} |j, j\rangle \langle j, j| U_h^{(j)\dagger})], \tag{23}$$

for the outcomes of the measurement described by the POVM $P_g^{(l)}$ at the output of the optimal stretching channel is exactly the same as that of $P_g^{(j)}$ at the input

$$q(g|h) = \text{Tr}[P_g^{(j)} U_h^{(j)} |j, j\rangle \langle j, j| U_h^{(j)\dagger}]. \tag{24}$$

Since the mutual information of the two random variables g, h is a functional of the conditional probability, $p(g|h) = q(g|h)$, this implies that the mutual information obtained by the POVM $P_g^{(j)}$ at the input is preserved at the output. Therefore, the optimal spin-stretching map preserves the mutual information.

For *qubits* the No-Cloning theorem is equivalent to the No-Stretching theorem. Indeed, perfect cloning from m to $n > m$ copies is equivalent to stretching the total angular momentum from $j = \frac{m}{2}$ to $l = \frac{n}{2}$. Moreover, the optimal fidelity for $m \rightarrow n$ cloning is given by [24]

$$F = \frac{m+1}{n+1}, \tag{25}$$

which coincides with Eq. 15. Clearly, No-Cloning for qubits implies No-Cloning for qudits. For qtrits or generally larger dimension $d > 2$, what

the No-Stretching theorems forbid is to transfer a group transformation covariantly to a system carrying more information about such transformation. However, this condition is harder to state in precise mathematical terms involving parameters of irreducible input and output representations.

In conclusion, we have seen that it is forbidden to stretch a spin while keeping its unknown orientation, a new no-go theorem which we call *No-Stretching Theorem*. We have seen that this is not due to conservation laws, since the transformation in the opposite direction—i. e. decreasing the angular momentum—is possible perfectly (this is non obvious). The No-Cloning theorem is a special case of the no-stretching Theorem, and for qubits the optimal spin-stretching $j \rightarrow l$ transformation coincides with the optimal cloning from $m = 2j$ to $n = 2l$ copies.

This work has been supported by the EC through the project CORNER.

References

- [1] Gernot Alber, Rottel, T. Beth, and M. Horodecki. *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2001.
- [2] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
- [3] R. Clifton, J. Bub, and H. Halvorson, Found. Phys. **33**, 1561 (2003).
- [4] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
- [5] D. Diecks, Phys. Lett. A **92**, 271 (1982).
- [6] H. P. Yuen, Phys. Lett. A **113**, 405 (1986).
- [7] A thorough account of the history of the no-cloning theorem can be found in Refs. [8, 9].
- [8] A. Peres, Fortschritte der Physik **51**, 458, (2003).
- [9] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín. Rev. Mod. Phys., **77**, 1225, (2005).
- [10] J. Fiurášek, M. Dušek, and R. Filip, Phys. Rev. Lett. **89**, 190401 (2002).
- [11] G. M. D’Ariano and P. Perinotti, Phys. Rev. Lett. **94**, 090401 (2005).

- [12] G. M. D'Ariano and P. Perinotti, in *Quantum Probability and Infinite Dimensional Analysis*, ed. by L. Accardi, W. Freudenberg, and M. Schürmann (World Scientific, Singapore, 2007), p. 173.
- [13] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, R2626 (1999).
- [14] F. De Martini, V. Bužek, F. Sciarrino, C. Sias, Nature **419**, 815 (2002).
- [15] This is the argument of the proof of the no-cloning theorem of Ref. [6], which is indeed more stringent than that of Ref. [4]. More precisely, in Ref. [4] it is shown that the cloning machine violates the superposition principle, which applies to a minimum total number of *three* states. In Ref. [6] it is shown that the machine would violate unitarity, which shows that any *two* nonorthogonal states cannot be cloned.
- [16] F. Buscemi, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Lett. A **314**, 374 (2003).
- [17] A. Messiah, *Quantum Mechanics*, North-Holland, New York (1962).
- [18] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Springer Verlag, Berlin, 1983.
- [19] M. Choi, Lin. Alg. and App. **10**, 285 (1975).
- [20] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
- [21] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
- [22] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, 1982.
- [23] G. Chiribella, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **72**, 042338 (2005).
- [24] R. Werner, Phys. Rev. A **58**, 1827 (1998).
- [25] E. B. Davies, IEEE Trans. Inform. Theory **5**, 596 (1978).